# NAVAL WAR COLLEGE

**Newport, R.I.**

## Applying Advances in Information Operations to Peace Enforcement

By

Marvin A. Englert
Lieutenant-Colonel, United States Army

As a Course Requirement

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements for the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Army.

Signature:____________________

18 May 2001

# Report Documentation Page

| | | |
|---|---|---|
| **Report Date**<br>18052001 | **Report Type**<br>N/A | **Dates Covered (from... to)**<br>- |

| | |
|---|---|
| **Title and Subtitle**<br>Applying Advanced in Information Operations to peace enforcement | **Contract Number** |
| | **Grant Number** |
| | **Program Element Number** |
| **Author(s)**<br>Englert, Marvin A. | **Project Number** |
| | **Task Number** |
| | **Work Unit Number** |
| **Performing Organization Name(s) and Address(es)**<br>Naval War College 686 Cushing Road Newport, RI 02841-1207 | **Performing Organization Report Number** |
| **Sponsoring/Monitoring Agency Name(s) and Address(es)** | **Sponsor/Monitor’s Acronym(s)** |
| | **Sponsor/Monitor’s Report Number(s)** |
| **Distribution/Availability Statement**<br>Approved for public release, distribution unlimited | |
| **Supplementary Notes** | |
| **Abstract** | |
| **Subject Terms** | |
| **Report Classification**<br>unclassified | **Classification of this page**<br>unclassified |
| **Classification of Abstract**<br>unclassified | **Limitation of Abstract**<br>UNLIMITED |
| **Number of Pages**<br>23 | |

## REPORT DOCUMENTATION PAGE

**1. Report Security Classification**: UNCLASSIFIED

**2. Security Classification Authority**:

**3. Declassification/Downgrading Schedule**:

**4. Distribution/Availability of Report**: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

**5. Name of Performing Organization**:
JOINT MILITARY OPERATIONS DEPARTMENT

| | |
|---|---|
| **6. Office Symbol**:<br>C | **7. Address**: NAVAL WAR COLLEGE<br>686 CUSHING ROAD<br>NEWPORT, RI 02841-1207 |

**8. Title** (Include Security Classification): Applying Advanced in Information Operations to peace enforcement (Unclassified)

**9. Personal Authors**: Lieutenant-Colonel Marvin A. Englert

| | |
|---|---|
| **10.Type of Report**: FINAL | **11. Date of Report**: 18 May 2001 |

**12.Page Count**: 22 **12A Paper Advisor (if any): Professor Milan N. Vego**

**13.Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

**14. Ten key words that relate to your paper**: Information Operations, Network-Centric Warfare, Army Battle Command System, Operation Joint Endeavor, Operation Joint Guard, Information Technologies, Peace Enforcement, Military Operations Other Than War, Interface, Integrate

**15.Abstract:** The Armed Services of the United States are experimenting with concepts that use recent advances in information technologies to enhance its information operations. Two of these concepts are Network-Centric Warfare and Army Battle Command System being developed by the United States Navy and the United States Army, respectively.

These concepts are being applied to enhance military operations in the combat environment. However, there is some question as to their usefulness in the Military Operations Other Than War (MOOTW) environment that the armed services will continue to be involved in.

This paper examines the applicability of these concepts to information operations in the MOOTW environment using the peace enforcement operation in Bosnia, *Joint Endeavor/Joint Guard*, as an example. It also examines the impact these developments may have on our allies, coalition partners, government and non-government organizations in this environment.

| | | | |
|---|---|---|---|
| **16.Distribution / Availability of Abstract:** | **Unclassified**<br>**X** | **Same As Rpt** | **DTIC Users** |

**17.Abstract Security Classification**: UNCLASSIFIED

**18.Name of Responsible Individual**: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

| | |
|---|---|
| **19.Telephone:** 841-6461 | **20.Office Symbol:** **C** |

**Security Classification of This Page** **Unclassified**

## Abstract

# Applying Advances in Information Operations to Peace Enforcement

The Armed Services of the United States are experimenting with concepts that use recent advances in information technologies to enhance its information operations. Two of these concepts are Network-Centric Warfare and Army Battle Command System being developed by the United States Navy and the United States Army, respectively.

These concepts are being applied to enhance military operations in the combat environment. However, there is some question as to their usefulness in the Military Operations Other Than War (MOOTW) environment that the armed services will continue to be involved in.

This paper examines the applicability of these concepts to information operations in the MOOTW environment using the peace enforcement operation in Bosnia, *Joint Endeavor/Joint Guard*, as an example. It also examines the impact these developments may have on our allies, coalition partners, government and non-government organizations in this environment.

## Thesis

**By integrating the United States Armed Services information systems used in our garrison, training and operational environments with available "off the shelf" items in the civilian sector to support the operational commander and their staff, Military Operations Other Than War (MOOTW), specifically Peace Enforcement Operations, can be greatly enhanced by applying concepts such as Network-Centric Warfare and Army Battle Command System to Information Operations**.

This thesis is relevant because there have been concerns that advances in information operations such as Network-Centric Warfare cannot be used in the peace enforcement environment because it is designed to lock-out the enemy's ability to effectively observe, orient, decide and act leading to paralysis and defeat of the enemy.[1] The same rationale would lead one to believe that our soldiers, sailors, airmen and marines cannot perform peace enforcement because they are trained to defeat their enemy counterparts. Just as service members can be trained to effectively accomplish assigned missions in the peace enforcement environment, the advances in information operations, such as Network-Centric Warfare, can be applied and have the same, if not greater, enhancement capability in the peace enforcement environment because it is a more permissive one to operate in. Additionally, included in the National Military Strategy are the objectives to "Promote Peace and Stability and, when necessary, to Defeat Adversaries," and the statements that "Our Armed Forces' foremost task is to fight and win our Nation's wars" and "The United States military will be called upon to respond to crisis across the full range of military operations, from humanitarian assistance to fighting and winning major theater wars…"[2] Therefore, any new concept which the armed services devote resources to should first support its foremost task – fight and win our Nation's wars. This paper will prove the thesis by providing examples of tasks assigned to the operational commander in the peace enforcement environment and the applicability of advances in information operations to being a force multiplier in accomplishing these tasks.

## **Preface**

"Information operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems."[3] The purpose of this paper is to show that advances in information operations such as the development of the concepts of Network-Centric Warfare by the United States Navy and the Army Battle Command System by the United States Army as it is being applied to current and future operations is not only applicable to combat, but also to Military Operations Other Than War (MOOTW). The armed services will continue to be involved in MOOTW; it will not focus on either defensive or offensive information operations but on the potential benefits that can be reaped by the operational commander by applying these concepts in the MOOTW environment. This paper will focus on one MOOTW mission, peace enforcement, throughout. Examples from the peace enforcement mission *Joint Endeavor/Joint Guard* in Bosnia will be used throughout this paper and are based on the author's eleven months experience in Bosnia. A description of the Network-Centric Warfare and Army Battle Command System concepts will be provided in more detail. This will be followed by examples of objectives and tasks (sub-objectives) the operational commander may have to achieve or support in the peace enforcement environment. Advances in information operations will be applied to each of these tasks to show how its application can enhance the ability of the operational commander(s) to achieve their mission(s). Finally, the impact these information operation advances may have on our allies, coalition partners, governmental and non-governmental organizations in the peace enforcement environment will be addressed.

## **Framework**

Rapid advances in information technologies have resulted in the United States Navy and Army to develop concepts such as Network-Centric Warfare and the Army Battle Command System, respectively, which take advantage of these developments. These concepts are described below.

"Network-Centric Warfare is a concept about means. It focuses on attaining access – access to gather, process and manage information to take advantage of the growing power resident in information networks."[4] Network-Centric Warfare is "Warfare which derives its power from the robust networking of a well informed and geographically dispersed force. Its enabling elements include: enhanced situational awareness, self-synchronization, increased speed of command, and distributed firepower for massed effect and greater efficiency. It is based on human behavior and is about generating an information advantage and translating it to a competitive advantage."[5] Network-Centric Warfare enables the operational commander get inside the enemies decision cycle through superior information processing and rapid decision making. At its extreme, Network-Centric Warfare can, through increased speed of command, enable the operational commander to virtually paralyze the enemy's ability to act thus leading to the enemy's defeat. Additionally, since all commanders and their staffs share or have access to the same information, in near real-time, they are able to self-synchronize in changing situations.

Likewise, the Army's Battle Command System "capitalizes on the power of our quality soldiers, enabled by what we now call Information-Age technology and permits commanders at every level to share a common, relevant picture of the battlefield scaled to their level of interest and tailored to their special needs."[6] All the attributes that apply to the Navy's Network-Centric Warfare, described above, apply to the Army's Battle Command System.

Both of these concepts represent considerable advances in information operations and can be accomplished by properly interfacing the technical command and control, communications, computer, intelligence, surveillance and reconnaissance systems that exist today so that they provide useful information to the operational commander.

## **Operational Objectives**

The challenge for the Joint Task Force Commander (JTFC) in a peace operations environment is ensuring that "military/security, humanitarian/economic, and political/diplomatic activities are constantly coordinated."[7] Using the peace enforcement Operation *Joint Endeavor/ Joint Guard* as an example, the Dayton Agreement that brought an end to hostilities in Bosnia-Herzegovina set forth four operational objectives to be accomplished: "Provide security for the people of Bosnia; create a unified, democratic Bosnia within internationally recognized boundaries; rebuild the economy; and ensure the right of people to return to their homes."[8] As can be seen, only one of these objectives, provide security for the people of Bosnia, is clearly in the military domain. The operational tasks which the JTFC must accomplish in regards to providing security for the people of Bosnia are to “maintain the cease-fire, separate forces and undertake arms control.”[9] However, if the CJTF does not accomplish the assigned military tasks progress towards meeting the other operational objectives may be impossible because their accomplishment depends on a secure environment. For example, if opposing Bosnian, Serb and Croat forces were not separated and confined to cantonment areas it would be impossible to erase the internal, artificial boundaries that had resulted from the civil war within Bosnia; if the military could not provide a secure environment, the people of Bosnia would not have an incentive to rebuild their infrastructure and homes and more importantly external international investors, government and independent, would not risk their resources to help the Bosnian economy; without a secure environment the Bosnians cannot return to their homes of origin if they had lived in other ethnically dominated areas.

In the Peace Enforcement environment it is the Operational Commander who sets the conditions for success by providing a secure environment in which governmental and non-governmental agencies can work to bring about a lasting peace.

## Network-Centric Warfare/Army Battle Command System Supported Information Operations

**Maintain cease-fire.** The first tasks assigned the operational commander in Bosnia for Operation *Joint Endeavor/Joint Guard* were maintaining the cease-fire and separating opposing forces. Initially, maintaining the cease-fire was accomplished by employing a credible, overwhelming international Combined Joint Task Force (CJTF) into Bosnia. This did not prevent the occasional fires from the opposing forces directed against each other prior to their separation, but it did prevent them from engaging peace enforcement units with hostile fire. The long-term task of maintaining the cease-fire over time was accomplished by maintaining a credible deterrent force in Bosnia as well as constant patrolling of each sector to ensure cease-fire compliance. There are several systems available that exist or are under development that, if interfaced through the application of Network-Centric Warfare or the Army Battle Command System, could enhance the effectiveness of these patrols and increase their force protection through increased situational awareness and speed of command. During Operation *Joint Guard*, a decision or lack there of, was reached regarding the sovereignty of Brcko, a key city on the Sava River, and the loss of which would cut the Serb community in Bosnia in half. The result was immediate, but not lasting, civilian hostility towards peace enforcers in the highly nationalistic cities of Brcko, Zvornik, Han Pijesak, and others. In fact, one psychological operations patrol, while operating in Zvornik, was attacked by Serbs armed with clubs who had been drinking at a local bar. The result was the peace enforcers, fearing for their lives, shot and killed one of the Serb assailants. This patrol was unaware of the recent decision concerning the status of Brcko. The application of Network-Centric Warfare or Army Battle Command System could have prevented this incident because the CJTF, being the first to know about these political decisions and linked by a common digitized maneuver control system from the tactical to operational level, could have provided subordinate commanders, with troops in high risk areas, immediate and specific warning and guidance. Subordinate commanders could then either decide to increase the protection of their forces in these areas or temporarily withdraw them until civilian hostility subsided. The United States Army is developing such a maneuver control system that is being tested at Fort Hood, Texas which provides locations of each element of a unit and overlays it on computer generated maps and graphics; this system provides leaders at every level a common operational picture of friendly forces.[10] This system greatly enhances speed of command, situational awareness, and self-synchronization.

**Separating opposing forces**. There were several difficulties encountered while attempting to achieve the separation of opposing forces: identification of opposing force commanders and units engaged, tracking withdrawing forces to approved cantonment areas outside of the zone of separation, and the scorched earth policy of opposing forces that were leaving areas they knew would be turned over to the other side. Compounding these difficulties was the geographically dispersed, non-linear battlespace the peace enforcers operated in.

The identification of opposing force commanders and their units could have been accomplished much more quickly and efficiently using Network-Centric Warfare or the Army Battle Command System. This was a critical implied task that had to be accomplished in order to separate the opposing forces because the peace enforcement commanders had to know who had the authority and responsibility to move these forces out of the Zone of Separation (ZOS). Although this problem was solved using traditional voice reporting systems at both the tactical and operational levels, it would have been accomplished much more quickly and efficiently using Network-Centric Warfare or the Army Battle Command System concepts. For example, if peace enforcement commanders at all levels were able to work together building a common, shared digital database, this implied task would have been accomplished much more quickly. Tactical units were working this from the bottom up while the JTFC and his staff was attaining this information from the top down.  A common, shared data base not only would have enhanced this process and facilitated the separation of forces, but would have provided operations and intelligence officers redundancy in verifying the accuracy of this information.

The tracking of withdrawing forces to approved cantonment areas outside of the Zone of Separation would also have been enhanced using these concepts.  This implied task was accomplished using traditional voice reporting systems and then transferring this information to maps and intelligence databases at each level of command.  Obviously, if this information could have been transmitted digitally in graphic format, as it was confirmed by the tactical level unit on the ground, a great deal of time would have been saved as well as providing commanders at both the tactical and operational levels a tremendously clear picture as to what was occurring on the ground.  The aforementioned maneuver control system provides the operational commander this capability.

The scorched earth policy adopted by opposing forces that were leaving areas that being turned over to the other side was an unforeseen and unanticipated development during the separation of forces.  In several instances, if the opposing force knew the area they were leaving was destined to be turned over to their former enemies, they would burn or booby-trap the homes with mines, ultimately resulting in additional hardship, and in some cases the death of innocent civilians returning to these homes.  For the tactical units involved, at first, these appeared to be isolated instances; however, it was discovered, some time later, that this was occurring throughout Bosnia.  This, as it turned out, was an operational issue that only the JTFC could resolve.  The reason this was an operational issue is because the peace enforcers, used to operating in a centrally planned/decentrally executed mission environment, were dealing with opposing forces who operated in a centrally planned/centrally controlled environment. Therefore, this required the involvement of the operational commander to solve. The speed of command that is provided through the concept of Network-Centric Warfare or the Army Battle Command System would have facilitated the identification of this problem through pattern analysis much sooner and thus saved property and lives.

The geographically dispersed, non-linear battlespace the peace enforcer had to operate in presented another challenge. In this environment the area between base camps could never be considered secure and in cases where combat force was required to compel compliance with the peace accords its effects had to be massed rapidly. This is exactly what concepts such as Network-Centric warfare are designed to facilitate, "distributed firepower for massed effect and greater efficiency."[11] Additionally in this environment, the use of video teleconferencing and electronic mail would enable commanders at all levels to conduct face-to-face meetings and coordination without having to travel to a specific location. This saves commanders time and the physical wear and tear resulting from travel; less travel also means less exposure that equates to increased forced protection. Video teleconferencing was used with great success during operations in Kosovo.[12] Operational logistics in the geographically dispersed, non-linear peace enforcement environment can also be greatly enhanced by implementation of concepts such as the Army Battle Command System through the use of radio frequency tags, shared data bases, automatic demand based resupply and establishment of a hub and spoke distribution system. The Army Battle Command System includes the Combat Service Support Control System, being tested at Fort Hood, Texas that does exactly this.[13] Many facets of this logistics system began to be implemented during operation *Joint Endeavor/Joint Guard* and many, if not all, of these ideas are drawn from examples in the civilian economic sector.

**Arms control**. The other major task assigned to the JTFC was to monitor arms control. This task involved consolidating heavy weapons such as tanks, armored personnel carriers, artillery (cannon and air defense), and heavy machine guns and grenade launchers into approved, by peace enforcement commanders, storage facilities. Likewise, troops were returned to cantonment areas with only individual weapons. Part of the challenge faced by the opposing forces was finding storage facilities and cantonment areas where none had existed before; however, this was their responsibility and they used open fields to store heavy equipment and abandoned schools and other facilities as cantonment areas. The challenge for the peace enforcers was inventory of equipment and approving/monitoring individual training of opposing force soldiers. Equipment found which was not in the proper place or on the inventory was confiscated and demilitarized; this included heavy combat vehicles. Weapons storage facilities and cantonment areas were required to be inspected and inventoried monthly and always subject to random inspections. Two problems were encountered during this process. First, there were times opposing forces personnel would not grant access to a facility by giving a wide range of excuses, such as it needed to be coordinated ahead of time or they had received orders not to allow access. In this case force was authorized to gain access, however, one of the principles of MOOTW is restraint and all other means were employed to gain access.[14] The end result was that access was granted, but sometimes not without the credible threat of overwhelming force and involvement of the JTFC. The other problem was a discrepancy with the weapons inventory. The discrepancies included excess weapons that were confiscated and missing weapons. Missing weapons required accountability and until they were found. The storage site or cantonment area was in a “red” status and the issue went through successive echelons of command until the appropriate opposing force response was garnered. Once again, the concepts of Network-Centric Warfare and Army Battle Command System apply in these cases. A digital reporting system to a common, shared data base at all levels would assist every level of command in early identification of problem areas which, when dealing with a centrally planned/centrally executed opposing force, requires the rapid involvement of the operational commander and perhaps civilian political involvement to avert the use of force. The enabling elements that enhance the execution of undertaking arms control task are, once again, enhanced situational awareness, increased speed of command and distributed firepower for massed effect and greater efficiency. An efficient means for sending and updating reports is computer electronic mail that enables reports and orders to be rapidly transmitted by digital means at the speed of light. Using commercially available software, any type of document can be sent by operational commanders and their staffs to subordinates and vice versa. Traditionally, these documents had to be sent by messenger or by unreliable and slow facsimile machines. Electronic mail combined with video teleconferencing greatly enhances parallel planning, the issuance of plans andorders and reporting. Also, the integration and interfacing of remote video systems can provide real time video information to the using headquarters. If these systems are properly interfaced with video teleconferencing, a single camera could provide real time video information to every level of command simultaneously. These capabilities further enhance speed of command and situational awareness. Examples of current systems are remotely piloted vehicles and fixed security cameras which could be used to monitor weapons storage facilities and cantonment areas around the clock decreasing inspection frequency by peace enforcers.

The bottom line is that Network-Centric Warfare and the Army Battle Command System both capitalize on the technological advances that have been made in the gathering of data by all sensor means and therefore turn this into useful information for the operational commander in near real-time because the digitized data can be moved and synthesized into usable information at the speed of light.[15] All of the above systems that have been used as examples must be linked and interfaced by robust, high capacity communications systems. Satellite communications are essential for units operating in non-linear, geographically dispersed areas with severe geographic features like those found in Bosnia. Communications, of all types, is the glue that holds all these systems together and facilitates the concepts of Network-Centric Warfare and the Army Battle Command System. These systems greatly enhance information operations and in turn become a common link between the operational factors of space, time and force. The operational space the commander has the ability to maneuver within has increased through the additional dimension of cyber-space.[16] Also, these same systems enable the operational commander to coordinate the activities of multiple units over great distances which is especially important in the peace enforcement environment where units are necessarily dispersed to accomplish their missions.[17] The operational factor time has gained increased significance by the sheer speed of data flow and information processing. Network-Centric Warfare and the Army Battle Command System will allow the operational commander to obtain information dominance regardless of the environment in which they are operating which ensures freedom of action at the expense of the enemy in combat or opposing forces in Peace Enforcement.[18] The operational factor force is greatly influenced by the amount of information available to everyone. The impact on the force is increased speed of command, greater efficiency in force deployments, more effective logistics.[19] One caution for the operational commander, especially in sensitive peace enforcement operations, is the amount of information available to the populace and media which can effect the MOOTW principle of legitimacy.[20] To control this the JTFC established a Joint Information Bureau (JIB) in Bosnia to guard against misinformation.[21]

As can be clearly seen, Network-Centric Warfare and the Army Battle Command System are as applicable in enhancing the capabilities of forces engaged in peace enforcement operations as they are in combat operations. The key to all of this is management and interfacing information technologies.

## Impact on Peace Enforcement Partners

One of the fears in both the combat and peace enforcement environment is that our allies and possible coalition partners will not be able to communicate with us because they cannot or are not keeping up with our advances in network-centric warfare concepts.[22] The solution to this problem is designing an open architecture that will facilitate unclassified access and provide Network-Centric Warfare and Army Battle Command System packages to our allies and coalition partners during combined operations.

As was previously stated, only one of the three operational objectives set forth in the Dayton Accords was the responsibility of the military. The other three operational objectives were to be accomplished by a combination of governmental and non-governmental organizations.[23] Therefore, it is essential that the operational commander be prepared to support and assist the efforts of these organizations in accomplishing their objectives. In order to do this, operational commanders normally establish a Civil Military Operations Center (CMOC) where the activities of these organizations can be coordinated with those of the military who is providing the secure environment in which they can accomplish their tasks in the peace enforcement or post-hostilities environment.[24] Additionally, each of these organizations is an additional sensor on the ground that can be used by the operational commander to gather information in the theater of operation. Therefore, for the increased security of these governmental and non-governmental organizations, unclassified access packages of network-centric warfare concept equipment should be available and offered for their use.

The synergistic effect of including allies, coalition partners, and governmental and non-governmental organizations into our networks would further enhance the ability of the JTFC to accomplish tasks in the Peace Enforcement environment.

## Conclusions

As can be seen, the concepts of Network-Centric Warfare and the Army Battle Command System not only apply in the combat environment, but may be even more beneficial to the JTFC in a peace enforcement environment. These concepts have the ability to provide an exponential increase in the quantity and quality of information available to the operational commander. This is not only beneficial in making sound decisions, but also in rapidly isolating and controlling incidents that occur in a highly sensitive peace enforcement environment before these incidents can adversely affect national/international strategic goals. Specifically, these concepts decrease the negative impacts of the factor of time and space and makes units more efficient and effective therefore requiring fewer units to accomplish the same tasks. Harnessing our information technologies for the operational commander is key to our National Security Strategy (NSS), a strategy that will probably continue to involve United States' forces in peace enforcement operations, as well as requiring these same forces to continue shouldering the responsibility for world security.

## **Recommendations**

- Continue to focus on developing the concepts of Network-Centric Warfare and the Army Battle Command System to support the high intensity combat environment because the primary mission of United States armed forces is to win our nation's wars.
- Design an open architecture that will permit unclassified access and design packages that can be given to our allies, coalition partners, governmental organizations and non-governmental organizations, as necessary and appropriate.
- Make this a joint effort. Each armed service is pursuing these concepts independently. Working together will have a synergistic effect that will allow the armed services to apply this concept sooner and at less cost.

## Notes

[1] Thomas P. Barnett, “The Seven Deadly Sins of Network-Centric Warfare.” Proceeedings, (December 1999): 3.

[2] Joint Chiefs of Staff, National Military Strategy of the United States of America, (Washington, DC: September 1997) 2,5.

[3] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998) I-1.

[4] VADM Arthur K Cebrowski, “Network-Centric Warfare: An Emerging Military Response to the Information Age,” Presentation, U.S. Naval War College, Newport, RI: 29 June 1999.

[5] Ibid.

[6] Department of the Army, Force XXI Operations, TRADOC Pam 525-5 (Fort Monroe, VA: 1 August 1994) 3-2 to 3-4.

[7] Joint Warfighting Center, Joint Task Force Commander’s Handbook for Peace Operations, (Fort Monroe, VA: 16 June 1997) xix.

[8] General Accounting Office, Bosnia Peace Operation: Progress Toward Achieving the Dayton Agreement’s Goals: Report to Committee on Foreign Relations, (Washington, DC: May 5, 1997) 23.

[9] Ibid., 23.

[10] Department of the Army, Force XXI Operations, TRADOC Pam 525-5 (Fort Monroe, VA: 1 August 1994) 3-2 to 3-4.

[11] Lescher, W. K., “Network-Centric Warfare: Is it Worth the Risk?’ Proceedings, (July 1999) 58.

[12] Department of Defense, Kosovo/Operation Allied Force After-Action Report: Report to Congress, (Washington DC: 31 January 2000) 46-51.

[13] Carl D. Bird III, “Bosnia: Does Force XXI Technology Solve the Operational Logistic Problems in Operations Other Than War?” (21 May 1998) 21-39.

[14] Department of the Army, Peace Operations, FM 100-23. (Washington, DC: 30 December 1994) 17.

[15] Michael D. Starry, “FM 100-6: Information Operations,” Military Review 4. (November-December 1996) 3.

[16] Milan N. Vego, Operational Warfare, NWC. (2000) 97.

[17] Ibid, 97.

[18] Ibid, 99.

[19] Ibid, 101.

[20] Joint Chiefs of Staff, Joint Doctrine for Joint Tactics, Techniques, and Procedures for Peace Operations, Joint Pub 3-08. (Washington, DC: 12 February 1999) I-7.

[21] Jeremy Shapiro, “Information and War: Is It a Revolution?” Strategic Appraisal. The Changing Role of Information in Warfare. (Santa Monica, CA: 1999) 125.

[22] David C. Gompert et al, Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs, (Washington DC: 1999) 3-4.

[23] General Accounting Office, Bosnia Peace Operation: Progress Toward Achieving the Dayton Agreement’s Goals, Report to Committee on Foreign Relations. (Washington, DC: 5 May 1997) 60-85, 102-143.

[24] Joint Chiefs of Staff, Joint Doctrine for Interagency Coordination During Joint Operations, Joint Pub 3-08. (Washington, DC: 9 October 1996) III-16 to III-19.

## Bibliography

Alberts, David S., et al., Network Centric Warfare:Developing and Leveraging Information Superiority, 2nd Edition (Revised).

Barnett, Thomas P., "The Seven Deadly Sins of Network-Centric Warfare." Proceeedings, December 1999.

Bird, Carl D. III, "Bosnia: Does Force XXI Technology Solve the Operational Logistic Problems in Operations Other Than War?" May 21, 1998.

Boorujy, James R., "Network-Centric Concepts Can Guarantee Access." Proceedings, May 2000.

Campbell, Spencer J., et al., "Operation Joint Guard (SFOR) Bosnia: Assessment of Operational Stress and Adaptive Coping Mechanisms of Soldiers." March 4, 1998.

Caneva, Joseph W., "Network-Centric Warfare: Implications for Applying the Principles of War." May 17, 1999.

Cebrowski, A. K., et al., "Network-Centric Warfare: Its Origin and Future." Proceedings, January 1998.

Cebrowski, A. K., "Network-Centric Warfare: An Emerging Military Response to the Information Age." Presentation. U.S. Naval War College, Newport, RI: 29 June 1999.

Dawson, J. Cutler, et al., "The IT-21 Advantage.' Proceedings, December 1999.

General Accounting Office, Bosnia Peace Operation: Mission, Structure, and Transition Strategy of NATO's Stabilization Force. Report to Committee on Foreign Relations. Washington, DC: October 8, 1998.

General Accounting Office, Bosnia Peace Operation: Pace of Implementing Dayton Accelerated as International Involvement Increased. Report to Committee on Foreign Relations. Washington, DC: June 5, 1998.

General Accounting Office, Bosnia Peace Operation: Progress Toward Achieving the Dayton Agreement's Goals. Report to Committee on Foreign Relations. Washington, DC: May 5, 1997.

Gompert, David C. et al, Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs, Washington DC: 1999.

Headquarters, Department of the Army, Force XXI Operations. TRADOC Pam 525-5. Fort Monroe, VA: August 1, 1994.

Headquarters, Department of the Army, Peace Operations. FM 100-23. Washington, DC: December 30, 1994.

Johnstone-Burt, “IFOR’s C4I and Information Operations: A Multinational Perspective.” July 1997.

Lescher, W. K., “Network-Centric Warfare: Is it Worth the Risk?’ Proceedings, July 1999, pp. 58-63.

Mace, Patrick D., “The Dayton Accord: Defining Success.” April 17, 1996.

_________, “Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age” (draft).

Shapiro, Jeremy, “Information and War: Is It a Revolution?” Zalmay M. Khalilzad and John P. White, editors, Strategic Appraisal. The Changing Role of Information in Warfare. Santa Monica, CA: RAND Corporation, 1999.

Starry, Michael D., “FM 100-6: Information Operations,” Military Review 4. November-December 1996.

U.S. Department of Defense, Kosovo/Operation Allied Force After-Action Report: Report to Congress, Washington DC: 31 January 2000.

U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: 9 October 1998.

U.S. Joint Chiefs of Staff, Joint Doctrine for Interagency Coordination During Joint Operations. Joint Pub 3-08. Washington, DC: 9 October 1996.

U.S. Joint Chiefs of Staff, Joint Doctrine for Joint Tactics, Techniques, and Procedures for Peace Operations. Joint Pub 3-08. Washington, DC: 12 February 1999.

U.S. Joint Chiefs of Staff, National Military Strategy of the United States of America. Washington, DC: September 1997.

U.S. Joint Warfighting Center, Joint Task Force Commander’s Handbook for Peace Operations. Fort Monroe, VA: 16 June 1997.

U.S. White House, A National Security Strategy for a New Century. Washington, DC: December 1999.

Vego, Milan N., Operational Warfare .  NWC, 2000.

Zimm, Alan, D., “Human-Centric Warfare.” Proceedings, May 1999, pp. 28-31.